ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●昨年摘発の中継サーバに1800万人分のアカウント情報、うち1割で不正接続確認･･･警視庁発表

http://www.nikkei.com/article/DGXLZO98851910V20C16A3CC0000/
http://www.yomiuri.co.jp/national/20160325-OYT1T50094.html

このニュースをザックリ言うと･･･

- 3月25日（日本時間）、警視庁サイバー犯罪対策課は、昨年11月に摘発した都内サーバ業者のプロキシ(中継)サーバから、ネット利用者のべ1800万人分のアカウント情報（ID・パスワード）が見つかったと発表しました。

- サーバ業者の摘発容疑は、中国の利用客に対しこれらのアカウント情報による不正接続を提供していたというもので、確認されたアカウント情報は「Yahoo!」「楽天」「Twitter」「Apple」など国内外31社のサイトにわたっており、うち1割にあたる178万件については実際に不正アクセスに成功したとされています。

- 警視庁は2014年にも別のサーバ業者を摘発しており、その際約506万人分のアカウント情報を確認していましたが、今回はその3倍以上となり、これほどの例は初めてだとしています。

AUS便りからの所感等

- サーバに保存されていたアカウント情報の多くは、他のサービスへの不正アクセスによって奪取されたアカウントと同じID・パスワードを使い回していた可能性が考えられます。

- 可能な限り、サービスごとに異なる、かつ推測されにくいパスワードを設定することが重要であり、自分にしかわからない法則性を決めてパスワードを設定することや、あるいは場合によってはパスワード管理ツールを導入することも検討に値するでしょう。

- この他では、マルウェアの感染やフィッシングサイトへの誘導により入手されたケースも考えられ、こういった経路でのアカウント情報の流出を避けるため、アンチウイルスやUTMの導入およびブラウザ等のアンチフィッシング機能の活用が重要です。

日本経済新聞

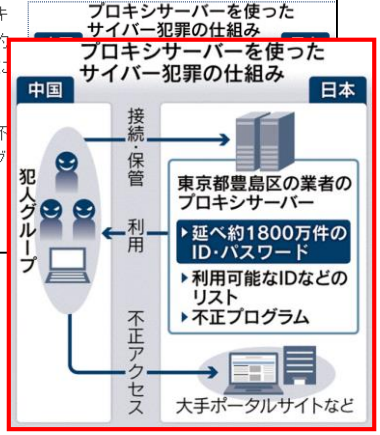
不正アクセス事件、警視庁押収のサーバーに個人情報1800万件
サイト侵入の温床に
2016/3/25 13:41

小 中 大 保存 印刷 リプリント 共有

インターネット接続を中継する「プロキシサーバー」の運営業者らが昨年11月に摘発された不正アクセス事件で、警視庁サイバー犯罪対策課は25日、押収した東京都豊島区の業者のサーバーから、大手ポータルサイトなどのIDやパスワード延べ約1800万件が見つかったと発表した。

同課によると、これほど大量の個人情報がプロキシサーバーから見つかったのは初めて。このうち約178万件のIDやパスワードは実際に不正アクセスに成功したとしてリスト化されていた。

一部のサイトではポイントの不正使用や商品の不正購入などの被害が確認された。同課は中国のグループが、不正入手した大量の個人情報をサーバーに保管・蓄積し、それを使って様々なサイトに侵入し、サイバー犯罪を試みていたとみている。



YOMIURI ONLINE

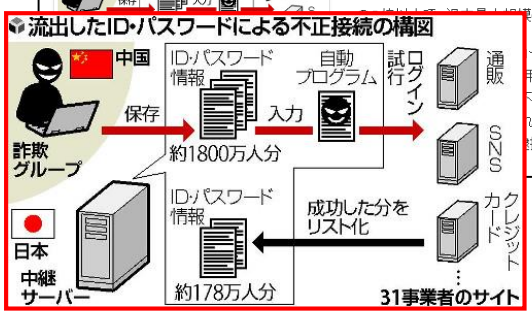
1800万人分のID流出…1割で不正接続確認

2016年03月25日 13時31分 ツイート おすすめ 706 G+1 19 B! 47

中国向けの中継サーバーがインターネットの不正接続に使われた事件で、警視庁は25日、昨年11月に摘発した東京都内の業者のサーバーから、ネット利用者延べ約1800万人分のIDやパスワードが見つかったと発表した。

このうち約178万人分は「ヤフージャパン」や「楽天」「ツイッター」などの会員情報で、パスワードなどを使った不正接続が確認された。同時期にポイントが不正利用されるなどの被害が出ており、同庁が捜査している。

中継サーバーを巡っては、同庁が2014年に摘発した別の業者のサーバーから約506万人分のIDなどが見つかっている。今回はその3倍以上の流出となる。



●2015年の標的型メール攻撃、過去最多の3828件・・・警察庁発表

http://securityblog.jp/news/20160330.html

このニュースをザックリ言うと・・・

- 3月17日（日本時間）、警察庁より、「平成27年におけるサイバー空間をめぐる脅威の情勢について」の発表がありました。

- 同年に警察が連携事業者等から報告を受けた標的型メール攻撃は3,828件と過去最多で、これは平成26年の1,723件の倍以上となっています。

- また、インターネットとの接続点に設置したセンサーに対する1日1IPアドレスあたりのアクセス件数は729.3件で、ルータ・監視カメラ等の組込み機器を標的とした探索行為等が増加した模様です。

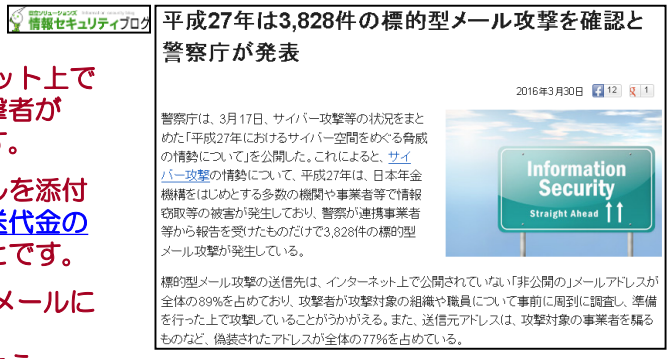
- この他、9月以降、地方公共団体・報道機関・空港・水族館等58組織のWebサイトが国際的クラッカー集団「Anonymous」によるとみられるDDoS攻撃で閲覧障害が発生した、等のトピックが挙げられています。

AUS便りからの所感等

- 標的型メール攻撃については、攻撃メールの89%がネット上で公開されていないメールアドレスあてのものとされ、攻撃者が周到な事前調査等をしていたことが伺えるとされています。

- また、53%が不正なマクロを含むWord形式のファイルを添付しており、多くは複合機からの文書スキャンデータや発送代金の請求のような業務上の連絡を装ったものであったとのことです。

- とにかく、アンチウイルスやUTM等による標的型攻撃メールに添付されたマルウェアに感染しないための防御策と、
万が一感染が発生した場合の情報流出を食い止められるよう、
やはりUTMの活用を含めたネットワーク構成の見直しの二方面からの対策が改めて求められます。


情報セキュリティブログ

平成27年は3,828件の標的型メール攻撃を確認と警察庁が発表

2016年3月30日

警察庁は、3月17日、サイバー攻撃等の状況をまとめた「平成27年におけるサイバー空間をめぐる脅威の情勢について」を公開した。これによると、サイバー攻撃の情勢について、平成27年は、日本年金機構をはじめとする多数の機関や事業者等で情報窃取等の被害が発生しており、警察が連携事業者等から報告を受けたものだけで3,828件の標的型メール攻撃が発生している。

標的型メール攻撃の送信先は、インターネット上で公開されていない「非公開の」メールアドレスが全体の89%を占めており、攻撃者が攻撃対象の組織や職員について事前に周到に調査し、準備を行った上で攻撃していることがうかがえる。また、送信元アドレスは、攻撃対象の事業者を騙るものなど、偽装されたアドレスが全体の77%を占めている。

●MBRを上書きし、PCの起動を妨害するランサムウェアを確認

http://www.itmedia.co.jp/enterprise/articles/1603/31/news061.html

このニュースをザックリ言うと・・・

- 3月下旬以降、PCの正常な起動を妨害する新手のランサムウェアが確認されたとして、セキュリティベンダー各社等が取り上げています。

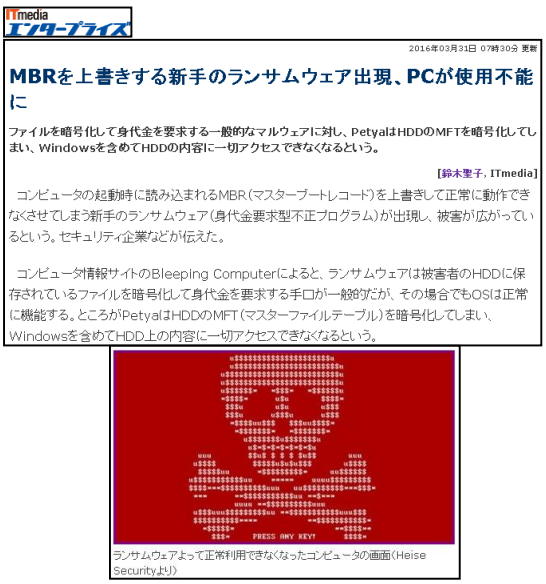
- 「PETYA」と名付けられたこのランサムウェアに感染すると、PCの起動時に読み込まれるMBR（マスターブートレコード）およびMFT（マスターファイルテーブル）が上書きされ、通常のOSの起動の代わりに、赤い背景に白いドクロのアスキーアートが表示されたうえ、ビットコイン（暗号通貨）による身代金の支払いが要求されます。

- 3月25日（現地時間）に米国のセキュリティ情報サイトBleeping Computerが取り上げた時点では「身代金を払う以外に暗号化の解除手段はない」とされていましたが、
その後3月29日にはドイツのセキュリティ企業
Heise Security社より、感染の最初の段階でのMBRの
暗号化は単純なものであると指摘がありました。

AUS便りからの所感等

- 幸いにも現時点ではPETYAによる暗号化の解除は可能な模様ですが、今後、より強力な暗号化を行う亜種が登場することが予想され、決して油断はできません。

- また、そういった亜種へのアンチウイルスやUTMの対応についてはタイムラグが生じる可能性もありますので、
単にそれらに依存するだけでなく、PCのOSや
各アプリケーションを最新に保つことも常に意識してください。


ITmedia エンタープライズ

2016年03月31日 07時30分 更新

MBRを上書きする新手のランサムウェア出現、PCが使用不能に

ファイルを暗号化して身代金を要求する一般的なマルウェアに対し、PetyaはHDDのMFTを暗号化してしまい、Windowsを含めてHDDの内容に一切アクセスできなくなるという。

[鈴木聖子, ITmedia]

コンピュータの起動時に読み込まれるMBR（マスターブートレコード）を上書きして正常に動作できなくさせてしまう新手のランサムウェア（身代金要求型不正プログラム）が出現し、被害が広がっているという。セキュリティ企業などが伝えた。

コンピュータ対策サイトのBleeping Computerによると、ランサムウェアは被害者のHDDに保存されているファイルを暗号化して身代金を要求する手口が一般的だが、その場合でもOSは正常に機能する。ところがPetyaはHDDのMFT（マスターファイルテーブル）を暗号化してしまい、Windowsを含めてHDD上の内容に一切アクセスできなくなるという。

ランサムウェアよって正常利用できなくなったコンピュータの画面（Heise Securityより）